The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

07/08/2014

SUBJECT:

Vulnerability in Windows Journal Could Allow Remote Code Execution (MS14-038)

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Windows Journal that could allow for remote code execution. Windows Journal is a note taking application that allows users to take handwritten notes on a tablet pc. This application is installed by default on all Windows systems other than Windows Server 2008. This vulnerability can be exploited when a user opens a specially crafted Journal file.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

At this time, there is no known proof-of-concept code available.

SYSTEM AFFECTED:

- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A vulnerability has been discovered in Windows Journal that could allow a remote attacker to take complete control of a vulnerable system. This vulnerability is caused by the way Windows Journal parses Journal files. The vulnerability could be exploited if a user opens a specially crafted Journal file.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/library/security/MS14-038

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1824